

PRINTER RUSH

(PTO ASSISTANCE)

Application : 09/603355 Examiner : Sam, P GAU : 2661

From : LC Location : IDC FMF FDC Date : 12/17/04

Tracking # : 06037503 Week Date : 11/18/04

DOC CODE	DOC DATE	MISCELLANEOUS
<input type="checkbox"/> 1449		<input type="checkbox"/> Continuing Data
<input type="checkbox"/> IDS		<input type="checkbox"/> Foreign Priority
<input checked="" type="checkbox"/> <u>CLM</u>	<u>09.15.2004</u>	<input type="checkbox"/> Document Legibility
<input type="checkbox"/> IIFW		<input type="checkbox"/> Fees
<input type="checkbox"/> SRFW		<input type="checkbox"/> Other
<input type="checkbox"/> DRW		
<input type="checkbox"/> OATH		
<input type="checkbox"/> 312		
<input type="checkbox"/> SPEC		

DIRECTOR OFFICE
TECHNOLOGY CENTER 2600

DEC 27 2004

RECEIVED

[RUSH] MESSAGE: Improper Dependency: Original Claim 28 depends on cancelled
original claim 23 Please Resolve

Thank You,
JS

[XRUSH] RESPONSE: Discussed this error with Mr. Lindsay Co.
McGuinness, attorney for applicant(s) on 1/18/05. She requests
the examiner, Phina Sam to correct this error by examiner's
amendment. Therefore, claim 28 should depend on claim 22.

P. Sam

INITIALS:

NOTE: This form will be included as part of the official USPTO record, with the Response document coded as XRUSH.

REV 10/04

Serial No. 09/603355

- 5 -

Art Unit: 2661

22. (original) A method of switching traffic in a packet-switched network having a plurality of nodes interconnected by links, the method comprising the steps of:

upon detection of a failure of a link connecting a pair of adjacent nodes, encapsulating packets within the bodies of tunnel packets and forwarding the tunnel packets along a predefined protection path which bypasses the failed link, including upon receipt of a tunnel packet by one of the adjacent nodes along a protection path, the recipient node retrieving the encapsulated packet and routing it as a function of a destination specified in the header of the encapsulated packet.

23. (canceled).

24. (currently amended) A method as claimed in claim ~~22~~ 23, wherein each packet comprises a header specifying the identity of a source node and a destination node associated with the packet.

25. (original) A method as claimed in claim 24, wherein the source and destination nodes associated with each tunnel packet correspond to the nodes at either end of the protected link.

26. (original) A method as claimed in claim 24, wherein the header of each packet further specifies the nature of the packet as a tunnel packet or a non-tunnel packet.

27. (original) A method as claimed in claim 26, wherein the header of each tunnel packet specifies the identity of the protection path along which it is sent.

28. (original) A method as claimed in claim ²²~~23~~, wherein all packets are Internet protocol (IP) datagrams.

29. (original) A packet-switched network comprising a plurality of nodes interconnected by links, wherein pre-defined protection paths provide protection of a selected plurality of links and wherein adjacent nodes connected by a protected link are adapted to detect a failure of the